EMAIL ACCOUNT SEARCH WARRANT AFFIDAVIT

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

IN THE MATTER OF THE SEARCH OF INFO ASSOCIATED WITH HOTMAIL EMAIL ACCOUNTS DESCRIBED IN ATTACHMENT "A" AND STORED AT PREMISES CONTROLLED BY MICROSOFT CORPORATION	Case No. 2:24-mj-01111 DBP **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Travis J Smoot, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Microsoft Corporation, an email provider headquartered at One Microsoft Way, Redmond, WA 98052. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Microsoft Corporation to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Postal Inspector assigned to the U.S. Postal Inspection Service, Phoenix Division domiciled in Salt Lake City, Utah. I have been employed by the U.S. Postal Inspection

Service since February 2014. I have been trained and have experience in investigating crimes related to the U.S. Postal Service, including violations of Title 18, U.S.C. §§ 1343 (Wire Fraud) and 1341 (Mail Fraud). Through both my training and experience, I have learned that fraudsters often use the U.S. Postal Service, financial institutions, peer-to-peer transfers, cellular phones, computers, and online applications to effectuate their schemes.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. § 1029 (Access Device Fraud); § 1341 (Mail Fraud); § and 1343 (Wire Fraud) have been committed. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

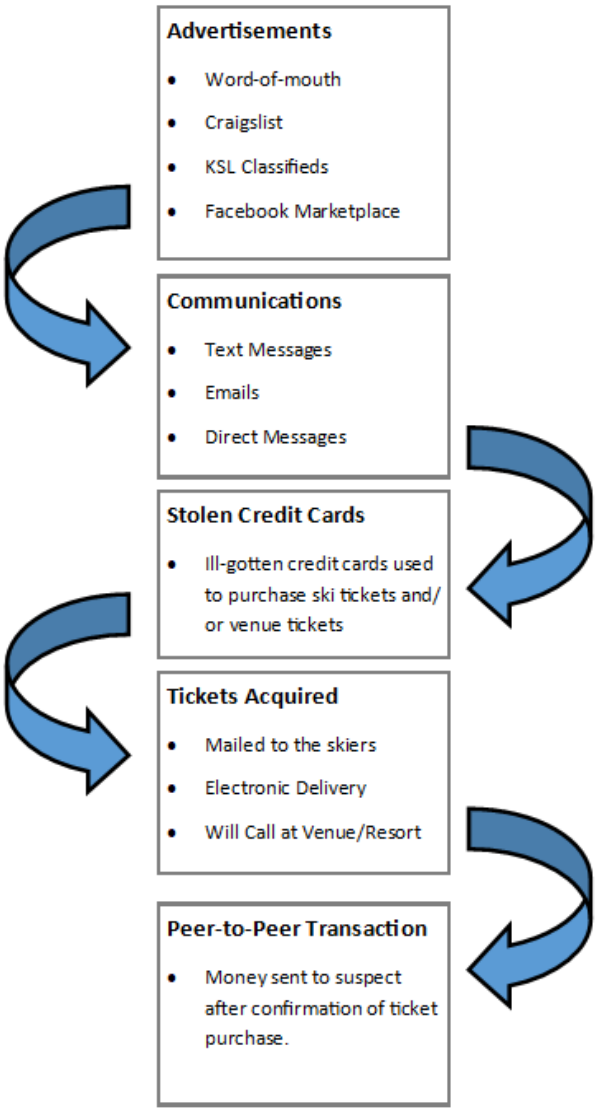
5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, this Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated."

OVERVIEW OF THE SCHEME

6. Beginning on a date unknown, but continuing between January 2020 and June 2024 a scheme to defraud individuals, businesses, and financial institutions was developed and perpetuated by individual(s) throughout the United States. The scheme was to purposefully defraud business(es) and/or individuals by selling ill-gotten tickets/passes via electronic means (text messages, social media, etc.).

7. The suspect(s) advertised discounted prices on tickets/passes to a variety of resorts/venues; communicated with victims wanting to purchase discounted tickets/passes; obtained the victim's name and address; unlawfully purchased tickets/passes with ill-gotten (stolen/compromised) bank card information; mailed or caused to be mailed tickets/passes purchased to the victims; and received peer-to-peer transactions (e.g. Zelle, Venmo, PayPal) from the victims to purchase the tickets/passes.

8. The following chart illustrates the scheme and method of operation:



9. The first element of the scheme involved the advertisement and/or promotion of discounted tickets (e.g. ski, concert). By means of word-of-mouth referrals, online classified marketplaces, and online social media platforms, victims were led to believe discounted tickets were available to purchase. These advertisements and communications offered by the suspect(s) via online promotion and/or telephone communications were in violation of Title 18 U.S.C 1343 (Wire Fraud).

10. The second element of the scheme occurred once the suspect(s) negotiated the specific ticket(s) and price. The suspect(s) then used stolen bank card information (including the bank card customer name(s), billing address(es), and bank card number(s)) to unlawfully purchase tickets in the name of the purchaser (e.g. skier). These transactions were done in violation of Title 18 U.S.C. 1029 (Access Device Fraud).

11. The third element of the scheme occurred after the unlawful bank card transaction was made (e.g. ski resort, concert venue). Once transacted, ticket(s) or pass(es) were issued and placed into the mail via the U.S. Postal Service ("USPS") and delivered to the purchaser(s). These mailings were used to further the scheme and were done in violation of Title 18 U.S.C. 1341 (Mail Fraud).

12. The fourth element of the scheme occurred once the unlawfully obtained ticket(s) were transacted. Once a confirmation number was available the suspect(s) used electronic communication methods (i.e. email, text messages) to communicate with victim(s) to send money via peer-to-peer network(s) (e.g. Zelle, Apple Cash, Venmo) to pay for the "discounted" ticket(s). The suspect(s) instructed the victim(s) to send money to specific user accounts by providing a username(s), handle(s), phone number(s), email address(es), etc. These accounts

were in control of the suspect(s) or their accomplices during the timeframe of the scheme. This was in violation to Title 18 U.S.C. 1343 (Wire Fraud).

13. Due to the complexity of the scheme, there are potentially four (4) separate intended victims per each transaction. The first victim is the bank card holder whose bank card was unlawfully used. The second victim is the bank card company. The third victim is the venue and/or resort (e.g. ski resort). The fourth victim is the individual who attempted to obtain the discounted ticket. At least one (1) of the victims listed above have sustained a loss as a result of the scheme.

14. During the investigation, some bank card customers notified their bank card company of the unauthorized charge on their account. These victims were able to successfully file an unauthorized/fraudulent dispute in relation to the transaction which then the bank card company (i.e. financial institution) sustained a loss. In some cases, the bank card company was able to successfully "charge back" the transaction to the vendor (e.g. ski resort). Note: A chargeback is a charge which is refunded to the account holder after the successful dispute of a transaction[1]. If the transaction was successfully charged back to the business (e.g. ski resort), the business sustained the financial loss. In some cases, the business (e.g. ski resort) was able to cancel the issued ticket(s) (e.g. ski pass). If the ticket/pass was cancelled, the purchaser (e.g. skier) sustained the loss from sending the payment via the peer-to-peer network (e.g. Zelle, Venmo, PayPal) to the suspect(s).

[1] Brady, S. (2024, January 24). *Credit card chargebacks: What are they and how do they work?* USA Today. https://www.usatoday.com/money/blueprint/credit-cards/credit-card-chargebacks/

15. The purpose of this affidavit is to provide the probable cause to show that the user account(s) were used in furtherance of the scheme to defraud financial institutions and individuals. It is believed the user account(s) allowed Jamilla Greene and others to facilitate and further the scheme and obfuscate their conduct and impede law enforcement efforts by creating layers of protection by using multiple phone numbers and email addresses.

16. The user account(s) listed in Attachment A has been specifically identified to have been used to further the scheme as one of the emails used to communicate with victims; linked to payment identifiers used via peer-to-peer transactions (e.g. Zelle, PayPal, Venmo); and/or used to store or save ill-gotten personally identifying information (PII) (e.g. credit cards). Thus the user-account(s) allowed the co-conspirators to facilitated the fraud scheme.

INVESTIGATION

Ski Resorts / Ski Passes

17. In March 2023, Brighton Ski Resort began looking into various chargebacks (credit card returns) during the ski-season and observed a high volume of chargebacks related to a user profile using their website. During their internal review, Brighton Ski Resort linked over $50,000 in chargebacks between January 2023 and April 2023. These ski passes were related to a ticketing portal user profile in the name “Jake Graham”; using the phone number 707-706-7676; and using the email address theskiinggawd@gmail.com. At least 30 chargebacks were observed with this same user profile.

18. On March 9, 2023, Brighton Ski Resort identified two individuals at their resort who were skiing under two of the passes purchased by the user “Jake Graham”. Brighton Ski Resort reported this to Unified Police and information was obtained from D.S. and E.J. surrounding the circumstances of the tickets they obtained.

19. The skiers, D.S. and E.J., explained they purchased the passes from "Jake" who had a phone number 980-202-2589. D.S. stated they received the name and phone number from a "friend-of-a-friend" who had previously purchased discounted passes through the same method. D.S. stated they contacted a person they believed to be "Jake" and through text messages arranged to purchase two discounted IKON ski passes around November 2022. D.S. provided to 'Jake" his and his wife's personal information needed to complete the IKON pass order including name, date of birth, address, and email address. Once he received from IKON the confirmation of the order, D.S. said he paid another individual as instructed by 'Jake'. The name of Jamilla Greene was given to D.S. He was told to pay the $610 (the discounted rate) per person. They stated they were instructed to send money through Venmo, PayPal, or Zelle. They were provided instructions to send $1,220 for two passes to the account of Jamilla Greene at j_greene03@icloud.com.

20. D.S. stated they sent the payment through PayPal and in December they received their IKON passes through the U.S. Mail. D.S. stated about one month later, the IKON pass was revoked and who received an email from Alterra Mountain Company (parent company of IKON) stating the credit card holder associated with the pass purchase had filed a dispute with the credit card company. D.S. contacted "Jake" regarding the revoked IKON pass and was offered an alternative option. The agreement was every time D.S. and E.J. wanted to ski, a ski pass would be provided by "Jake" at any ski resort in the United States. D.S. contacted "Jake" for ski passes for March 9, 2023 to ski at Brighton Ski Resort.

21. Brighton Ski Resort conducted an internal investigation into the online profile "Jake Graham" which had been used to purchase the day passes at the ski resort. The email address identified by Brighton Ski Resort was theskiinggawd@gmail.com.

22. Brighton Ski Resort reported the additional information to Unified Police Department which began an investigation into the fraudulent chargebacks and obtained various search warrants and subpoenas related to the users and accounts involved in the scheme. Detective Lenzer was able to identify email addresses, bank accounts, peer-to-peer transfer accounts, usernames, advertisements, phone numbers, and hundreds of compromised credit card numbers and personally identifying information of individuals.

23. Through these investigative efforts, investigators identified and spoke with another individual, C.S. C.S. stated he contacted "Jake" after receiving his name and phone number (980-202-2589) through a friend who had previously purchased discounted IKON passes. C.S. contacted Jake via phone and was instructed to provide money to Jamilla Greene in October 2022 through a PayPal account associated with j_greene03@icloud.com. C.S. stated he received an IKON pass through the mail and approximately one month later the pass was revoked for a "non-payment" issue. C.S. contacted "Jake" and was told the reason the IKON pass was revoked was due to a "batch" issue. C.S. was given an arrangement by "Jake" to obtain Brighton Ski Resort day passes to make up for the issue with the IKON ski pass being revoked.

24. Investigators identified two additional persons as K.G. and M.E. in relation to discounted ski passes. These passes were also flagged as part of the scheme related to "Jake Graham".

25. Investigators learned K.G. and M.E. had learned about the discounted ski passes from C.S. to purchase ski passes. K.G. and M.E. advised they were instructed to send money to a Venmo account belonging to user @millybx3 (Milly Bethea), later identified as Jamilla Greene. The passes were also charged back and revoked.

26. Investigators were able to follow-up on leads, conduct interviews, and obtain various legal processes which revealed additional information related to the scheme. The information they gathered included email addresses, bank accounts, peer-to-peer transfer accounts, usernames, advertisements, phone numbers, and hundreds of compromised credit card numbers and personally identifying information of individuals.

INVESTIGATION

980-202-2589

27. The investigation into the user "Jake Graham" and reports from the victims led investigators into seeking information related to the phone number 980-202-2589. The phone number resolved to Google Inc as the provider for this number. Note: Google Inc offers a variety of services within their domain including email (Gmail) and VoIP (Voice Over Internet Protocol) numbers (Google Voice).

28. A State of Utah search warrant (2639601) was obtained to identify the subscriber and user of 980-202-2589. The results of that warrant found that the number 980-202-2589 was associated with Gmail account jessiexduvalle@gmail.com. The subscriber information showed a name "Jessie Duvalle" a date of birth and recovery information which did not resolve to a specific person.

29. Another State of Utah search warrant (2664951) was issued related to the Google subscriber jessiexduvalle@gmail.com to review more aspects of the email account and user. Upon review of the entire Gmail user account, investigators identified various incoming and outgoing communications which appeared to be related to the fraud scheme. Investigators observed:

a. Multiple emails from cfeldbbc@aol.com which contained dozens of bank card numbers, names, addresses, and personally identifying information of individuals;

b. craigslist advertisements (listings);

c. Text messages (from the linked Google Voice account) regarding tickets/passes;

d. Voicemails from individuals related to tickets/passes; and

e. Emails referencing digital currency wallets.

30. At least 61 emails were sent/received by cfeldbbc@aol.com containing bank card information. Other emails to and/or from the account included j_greene03@icloud.com and agat741@aol.com.

31. One email of interest was a forwarded message from agat741@aol.com to jessiexduvalle@gmail.com on November 22, 2021. The message contained a forwarded message from hutchinstone@yahoo.com to agat741@aol.com on November 20, 2021. The subject of the email read "passes needing fixes asap".

32. The message continued with 23 lines of data for what appear to be "customers" of ski passes. Each line contains a name, birthdate, email address, mailing address, and the type of pass.

33. Investigators researched the bank card numbers found within the communications with cfeldbbc@aol.com and believed each of the bank card numbers and accompanying personally identifying information (PII) were stolen and/or compromised.

INVESTIGATION

CFELDBBC@AOL.COM

34. On November 20, 2023, a federal warrant (223mj1091) was issued by the U.S. Magistrate Judge in relation to information associated with the user-account CFELDBBC@AOL.COM.

35. Investigators reviewed the search warrant return from Yahoo and learned the subscriber information as follows:

a. Full Name: C Feld

b. Registration Date: 2014-05-10

c. Birthdate 1969-01-01

d. Recovery Emails: None

e. Recovery Phones: +16316334695 (verified 2023-11-22)

36. The emails found within the search warrant return do not show typical personal email traffic (i.e. junk mail, advertisements, subscriptions). The incoming emails found within the warrant show messages regarding craigslist posts for ski passes; digital currency wallet addresses; and credit card numbers and respective personally identifying information of said cardholders. Investigators believe there to be thousands of bankcard numbers within the correspondences found on cfeldbbc@aol.com, some of which were linked to the chargebacks identified by the ski resorts.

37. The majority of the email sender and recipient info is associated with the same address of cfeldbbc@aol.com. However, a few emails show forwarded emails (some with embedded emails) which identify the following associated email accounts:

f. futureisrisen@icloud.com

g. jessiexduvalle@gmail.com

h. blesshappyandloved@gmail.com

i. upsonold@magim.be

j. spurs13@mail.com

k. skiiaway1@hotmail.com

l. ikonpass22@yahoo.com

m. bright13@usa.com

38. These email addresses show correspondence continuing the fraud scheme by providing bank card information, personally identifying information, transaction receipts, invoices, or crypto currency wallets.

39. Investigators worked to identify the large amount of personally identifying information (PII), credit card numbers, and individuals whose information was found among the emails in the cfeldbbc@aol.com account. Investigators identified over 8,000 individuals PII among the emails during the search.

INVESTIGATION

SKIIAWAY1@HOTMAIL.COM

40. As previously mentioned, communications found within the account of cfeldbbc@aol.com found various email messages containing personally identifiable information of others.

41. An email message sent on January 3, 2021 from cfeldbbc@aol.com to skiiaway1@hotmail.com contained three bank card numbers and the associated personally identifying information related to the card holders.

42. A review of records obtained by investigators confirmed two of the three bank card numbers were used at Vail Resorts to purchase ski lift tickets. Further review found both the bank cards used resulted in a chargeback to the ski company.

INVESTIGATION

SKIIAWAY2@HOTMAIL.COM

43. The investigation led to seeking information related to Venmo user @rgreen06 (2023r00838-062). Victims reported sending money to the Venmo account to purchase discounted ski tickets. One victim, L.K., reported their interactions with the scheme and provided information related to a transaction sent to @rgreen06 via Venmo.

44. On or about August 17, 2023, L.K. was given the phone number 631-633-4695 to obtain discounted EPIC season ski passes. L.K. received a confirmation number and was instructed via message to send a peer-to-peer transaction to Venmo user @rgreen06. L.K. reported her EPIC season pass was later cancelled due to a fraudulent charge associated with the purchase. L.K. was unable to receive a refund and sustained a financial loss as a result of the scheme.

45. Investigators identified dozens of other similar transactions which were linked to charged back credit cards.

46. A review of the information (2023r00838-062) found information related to the subscriber of the account which is summarized below:

1. Name: R[redacted] Green
2. Date of Birth: [redacted]
3. SSN: [redacted]
4. Street Address: [redacted], Hawaii

5. Account Created: October 1, 2021

NOTE: R. Green is a true and living person who is not a subject of the investigation. The name, address, date of birth and other personally identifying information was found among the search warrant return associated with Jamilla Greene and appears to be unlawfully used to perpetrate additional financial schemes. The information is redacted to protect the true identity of the victim.

47. A review of the Venmo transactions associated with @rgreen06 found the transaction related to L.K. on June 25, 2022 for $435.00. Various comments on Venmo showed "lift", "Ski", "Ikon pass" and "Epic." A total of $217,785.48 was received into the Venmo account at $213,676.48 was sent from the account.

48. No financial accounts were linked to the account to allow for "deposits" or "withdrawals". This appears to be unusual as that many people would use Venmo to conduct peer-to-peer transactions and would fund their transfers from their linked bank account (i.e. bank account number, debit card number) to send funds. Also, accounts would be linked so a user could cash out (withdrawal) the funds from Venmo and place those funds into their banking account to be used.

49. The incoming funds were from various individuals which appear to be related to discounted ski passes and the transfers out of the account go to another Venmo account (120836026) referred to as R Mills and the email address skiiaway2@hotmail.com. A total of $77,422.79 was transferred to Mills.

50. During the course of the investigation, additional records related to Venmo account 120836026 (Mills) was requested and obtained (2023r00838-083). As previously mentioned, the Venmo account related to @rgreen06 had a significant amount of money coming

into the account which appeared to be related to fraudulent transactions and was immediately transferred to the Venmo account of Mills.

51. A review of the information (2023r00838-083) found information related to the subscriber of the account which is summarized below:

a. Name: R[redacted] Mills

b. Date of Birth: [redacted]

c. SSN: [redacted]

d. Street Address: [redacted], Hawaii

e. Account Created: January 25, 2022

f. Email Address: skiiaway2@hotmail.com

52. A review of the account transactions found a total of $206,667.50 received into the account and $200,316.87 withdrawn from the account. The comments associated with the transactions included “Airbnb”, “Appreciate You”, “Appreciation”, “Carnival week”, “Deductible”, “Parking”, “Pay me back”, “Rentals”, “Refund the money that was stolen from me from the number: 631-633-4695”, “The money that "[redacted] green" ph#631-633-4695 stole from me. Please tell him to pay me back.” among various other things including ski emojis.

53. Additionally, there was listed a JP Morgan Chase Bank debit card associated with the account. The debit card was listed as 4207670266970337. This would allow the Venmo account to fund and transfer funds to the linked JP Morgan Chase Bank account.

CONCLUSION

54. Based upon the supporting statements from victims; the information from Zelle (EWS); Venmo (PayPal Inc); the information from Craigslist Inc (craigslist); and the

investigation into the fraudulent scheme, it is believed that Jonathan Rembert and others are involved in violations related Title 18 USC 1029 (Access Device Fraud); Title 18 USC 1341 (Mail Fraud); and Title 18 USC 1343 (Wire Fraud). Based on the statements of the victims; the information from Venmo (PayPal), Zelle (EWS), and the investigation into the fraudulent scheme, it is believed that Jonathan Rembert, and others, are receiving ill-gotten proceeds and that evidence, fruits, instrumentalities, and/or proceeds will be found on communications associated with the email address(es) described in Attachment A.

55. In general, an email that is sent to a Hotmail or Outlook (Microsoft Corporation) subscriber is stored in the subscriber's "mail box" on Microsoft Corporation servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Microsoft Corporation servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Microsoft Corporation's servers for a certain period of time.

BACKGROUND CONCERNING EMAIL

56. In my training and experience, I have learned that Microsoft Corporation provides a variety of on-line services, including electronic mail ("email") access, to the public. Microsoft Corporation allows subscribers to obtain email accounts at the domain name hotmail.com or outlook.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Microsoft Corporation. During the registration process, Microsoft Corporation asks subscribers to provide basic personal information. Therefore, the computers of Microsoft Corporation are likely to contain stored electronic communications (including retrieved and unretrieved email for hotmail.com and/or outlook.com subscribers) and information concerning subscribers and their use of Microsoft Corporation services, such as account access information, email transaction information, and account application information. In my training and

experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

57. A hotmail.com and/or outlook.com subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, digitized images (other than ones attached to emails), and other files, on servers maintained and/or owned by Microsoft Corporation In my training and experience, evidence of criminal activity using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including images and files.

58. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

59. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage

of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

60. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

61. This application seeks a warrant to search all responsive records and information under the control of Microsoft Corporation, a provider subject to the jurisdiction of this court, regardless of where Microsoft Corporation has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Microsoft

Corporation's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States. [2]

62. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of the crime, or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account

---

[2] It is possible that Microsoft Corporation stores some portion of the information sought outside of the United States. In Microsoft Corp. v. United States, 2016 WL 3770056 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, and other courts have disagreed with the Second Circuit's conclusion, I respectfully request that this warrant apply to all responsive information— including data stored outside the United States—pertaining to the identified account that is in the possession, custody, or control of Microsoft Corporation *In re: Information associated with one Yahoo email address that is stored at premises controlled by Yahoo*, *In re: Two email accounts stored at Google Inc.*, Case No. 17–M–1234, Case No. 17–M–1235, 2017 WL 706307, (E.D. Wis. Feb. 21, 2017; *In re search warrant to Google,* 2017 WL 471564 (E.D.Pa. Feb. 3, 2017). The government also seeks the disclosure of the physical location or locations where the information is stored.

access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

63. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Microsoft Corporation, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Travis J. Smoot
U.S. Postal Inspector
United States Postal Inspection Service

Subscribed and sworn to before me on November 15, 2024

Honorable
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following accounts that are stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043.

- Skiiaway2@hotmail.com
- Skiiaway1@hotmail.com

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Microsoft Corporation (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. For the time period stated, the contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. For the time period stated, all records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. For the time period stated, all records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within **fourteen days** of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, U.S.C. §§ 1029 (Access Device Fraud), 1341 (Mail Fraud); 1343 (Wire Fraud), 1344 (Bank Fraud), those violations involving an persons known and unknown and occurring on a date unknown but continuing from January 7, 2020 through November 15, 2024, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Communications regarding accounts/relationships with financial institutions;

(b) Information regarding peer-to-peer transactions (i.e. PayPal, Venmo, CashApp, and digital currency);

(c) Lists, messages, files containing credit card numbers, personally identifying information of individuals, or other financial information related to individuals;

(d) Communications to/from individuals attempting to purchase, buy, sell, or negotiate tickets/passes;

(e) Communications regarding accounts opened/closed;

(f) Communications from resorts/venues (i.e. ski resorts, concert venues);

(g) Communications from vendors, companies, businesses regarding the advertisement, sale, or transfer of tickets, passes, or products;

(h) Communications regarding shipping or receiving of any mailings including tracking numbers;

(i) Communications from media companies (including social media companies) regarding the listing of tickets/passes;

(j) Images, links, texts, or files related to tickets, transactions, digital currency, crypto currency, and advertisements;

(k) Communications from Jamilla Greene and other co-conspirators;

(l) Evidence indicating how and when the email account was accessed or used for the dates of communications seized under sections (a) – (l) above, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(m) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation for the dates of communications seized under sections (a) – (l) above;

(n) The identity of the person(s) who created or used the user ID.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Microsoft Corporation, and my official title is _____. I am a custodian of records for Microsoft Corporation. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Microsoft Corporation, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Microsoft Corporation; and

c. such records were made by Microsoft Corporation as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature